SFO
SERIOUS FRAUD OFFICE
TE TARI HARA TĀWARE

Counter Fraud Centre
TAUĀRAI HARA TĀWARE

CASE STUDY - NOVEMBER 2024

Financial fraud to cover up theft of $225,000

The Counter Fraud Centre - Tauārai Hara Tāware (CFC) is the prevention arm of the Serious Fraud Office (SFO) and leads counter fraud efforts in New Zealand's public sector. Using actual cases prosecuted by the SFO, our case studies aim to help public organisations understand, identify and prevent the impact of fraud.

Use case studies to:

Case studies are useful to increase fraud awareness, by including them in online training modules or team discussions; to identify fraud risks, by considering whether the circumstances in this scenario might happen at your organisation; and to prevent fraud, by considering the controls that could prevent this fraud from occurring and implementing similar controls in your organisation.

In this case study:

Case information

After more than 20 years working for the New Zealand Defence Force (NZDF) in various roles, an employee was given sole responsibility for the financial management and reporting of a small number of non-public funds.

Non-public funds, established under section 58 of the Defence Act 1990, collectively operate as registered charities for each military service. The purpose of service and unit funds is to maintain the health, wellbeing and retention of NZDF personnel. The money for these funds is raised from NZDF personnel salaries and other fundraising activities. The funds are provided to various groups and clubs within the military generally.

The employee's responsibilities included depositing money into the funds' bank accounts. She did not bank all the cash received and instead used most of the unbanked cash for gambling. She had a gambling addiction and was spending around $500 per week on the pokie (slot) machines.

The offending occurred over a prolonged period without it being detected (at least seven years), because the employee was able to conceal the theft.

The theft was mainly concealed by:

1. Using a complicated cheque swap system. This involved taking funds from non-operating clubs to pay invoices of another club. The employee then wrote a cheque for the payment from the correct account but destroyed the cheque. This meant that the supplier was paid, and it appeared for all intents and purposes that the funds came out of the correct account.
2. The actual bank balances being less than the reported account balances in the cashbooks.

NZDF's Internal Audit conducted a review that looked at the non-public funds as a whole from an operating model and control framework perspective. The review identified control weaknesses including a lack of external audit, management oversight and a centralised accounting system.

NZDF management began a project to address the report recommendations and this activity led to the employee self-reporting the theft to her manager, who had been unaware of her offending.

This case was then referred to the Serious Fraud Office.

For more information about this case, you can find the SFO Media Release on our website.

Prosecution outcome

The employee pleaded guilty to one representative charge of "Theft by person in a special relationship" and one charge of "False accounting". She was sentenced to 12 months' home detention and 250 hours of community work.

The impact of the offending

- A detected financial loss of around $225,000.
- Reputational damage to the Defence Force.
- Fraudulent use of charitable funds diverted from their intended use, meaning the funds obtained were not available to support the wellbeing of NZDF personnel.
- NZDF incurred enquiry and response costs as a result of the fraud.

The organisation's response

- NZDF moved from manual to automated processes for managing the funds. The manual system required an employee to enter and reconcile the details in an Excel spreadsheet, whereas the automated system involves using an accounting software package.
- The NZDF business service and accounts team were restructured to create segregation of duties. Employees now work in a shared workspace and roles are shared to ensure oversight.
- NZDF conducted a Court of Inquiry to identify and reduce any future risk of fraud.

Strengthening counter fraud capability

- Does your organisation have sufficient segregation of duties for high fraud risk business processes? Cash management is usually considered a high fraud risk function.
- Do your employees understand how to perform quality assurance checks correctly and consistently? Are the outcomes of these checks followed up on?
- Does your organisation verify information with third parties where possible? Do your employees know what independent information is available for these checks?
- Are your policies and procedures clear about the documentation and signing requirements in support of a cheque payment?
- Does your organisation carry out reviews that can identify control weaknesses which could be exploited for fraud? Does your organisation act on the recommendations of these reviews?

Recognising common fraudster personas

There were three main personas in this case:

- **The Fabricator** – the employee was writing cheques then destroying them but making it appear as if they'd been presented for payment.
- **The Exploiter** - the employee used her position as an administrator to exploit a weakness in the internal controls.
- **The Deceiver** – the employee falsified the accounting records so that it appeared as if the funds in the bank accounts were higher than what they actually were.

For more information, you can find the fraudster persona guide on our website.

Red flags to watch out for

Whilst red flags don't necessarily indicate fraud, they can be a sign that something is out of the ordinary and may need to be looked into.

- **Employees who appear to have a lifestyle beyond their means** – the employee was spending a large amount on the pokie machines.
- **Processes not consistently being followed** – the employee received cash but didn't bank it straight away.
- **Lack of effective oversight** – the employee worked in isolation and didn't share duties. There was no oversight of what she was doing by anyone who understood what was required.
- **No segregation of duties** – the employee received the cash and reconciled the accounts. These should be separate functions.
- **Variances in record keeping** – cheques were recorded as presented to the bank, but bank statements didn't show this.
- **Unusual accounting practices** – cheques were being written for a club that was no longer operating. When other signatories were asked to countersign cheques, they did not question it.

Countermeasures to prevent and detect fraud

These are examples of countermeasures which could have been helpful in this instance:

- **Segregation of duties** – is where tasks for business processes are distributed among multiple staff. This reduces the chances of an employee being able to commit a fraudulent transaction and hide the nature of the transaction. Where segregation of duties isn't possible, due to the number of employees, more reliance should be placed on compensating controls such as quality assurance checks and external audits.
- **Quality assurance checks** – these are checks to confirm that processes are being followed correctly and to a high standard. The outcome of these checks needs to be followed up on to review any inconsistencies or concerns that may have been identified.

In the case of the non-public funds, the rules of the charity stipulated that periodic checks were to be carried out (by a checking officer) to ensure that the funds are being properly administered. The rules also provided that a supervising officer had to investigate any matters that the checking officer considered unsatisfactory.

- **Internal audits** – these are an objective review and assessment of the effectiveness of internal controls and risk management. In this case, the Internal Audit review identified significant control weaknesses which, when addressed, led to the employee self-reporting the theft. Regular internal audits can increase the fear of the fraud being exposed which can serve as a deterrent to committing fraud.

- **Ethical culture** – this is about creating a culture that encourages supportive behaviour. Health and wellbeing training initiatives around addiction and mental health can encourage staff to speak up and seek help.

- **Verifying information with third parties where possible** – this is done to verify key information with an independent and credible source. In this case, if the bank balances reported in the cash book had been verified against the bank statements, the overstatement in the cash book would have been detected.

For more information, you can find guides on our website for: capability countermeasures; prevention countermeasures; detection countermeasures and response countermeasures.

Need help?

Wherever you are with your counter fraud efforts, we're here to help.

We offer a range of resources to help build capability across your organisation. If you are in the public sector and would like to contact us about the services we can provide, please email counterfraud@sfo.govt.nz or visit www.sfo.govt.nz/counterfraud/cfc